U.S. Navy

The U.S. Navy Cyber Defense Operations Command (NCDOC) team suffered severe data overload from an ever-increasing number of security sensors, which issued steady streams of events and alerts. Carefully evaluating this flood of data would have required an estimated 8,820 additional security experts. NCDOC selected Sentinel for implementation of an automated, centralized security-event management system capable of handling tens of thousands of sensor-generated events and alerts daily across hundreds of geographically dispersed networks.

Overview
The NCDOC encompasses a small team of 180 security professionals charged with the big job of maintaining security for hundreds of U.S. Navy networks located around the globe in environments ranging from battle ships to regional headquarters.

Challenge
The NCDOC’s 180 personnel are responsible for analyzing huge volumes of network information from hundreds of locations worldwide—including ships, medical clinics, headquarters and research facilities. NCDOC monitors U.S. Navy networks 24 hours a day, 365 days a year and was experiencing data overload from an increasing number of cyber security sensors housed in a variety of network devices—including routers, intrusion detection systems and firewalls.

“We always choose the top tools in the industry, and Sentinel is a market leader.”

JIM GRANGER
Director of Capabilities and Readiness
Navy Cyber Defense Operations Command

Charged with carefully evaluating all network activity, but having insufficient personnel to do so, NCDOC sought to automate monitoring across its hundreds of security sensors. The solution had to be vendor-independent to accommodate a variety of platforms and systems, and scalable enough to handle continued growth in the number of sensors.

Solution
NCDOC created PROMETHEUS, a suite of tools that monitors, reports and thwarts malicious network activity. PROMETHEUS uses the SAS Intelligence Platform as its data warehouse back end, and NetIQ® Sentinel™ as its security-event management front end to monitor tens of thousands of network events every day.

“We always choose the top tools in the industry, and Sentinel is a market leader,” said Jim Granger, director of capabilities and readiness at NCDOC. “The product works well with SAS and met our requirements of being open and scalable.”

The PROMETHEUS system accesses and aggregates data from all portions of the network—including system, web, email, firewall and router logs—and prepares and stores the data for analysis and reporting. NetIQ Sentinel presents and prioritizes all security events in a centralized dashboard for security operators.

At a Glance

- Industry
  Government
- Location
  United States
- Challenge
  The lack of personnel to monitor many critical systems encouraged the NCDOC to seek an automated monitoring solution to cover hundreds of security sensors.
- Solution
  Use Sentinel as a security-event management front end to monitor tens of thousands of network events every day.
- Results
  + Automated and centralized security monitoring
  + Simplified daily reporting
“With Sentinel, we have a unified, real-time view of security activity across our diverse global environment from a central console,” said Keith Rohwer, NCDOC director of research, development, testing and evaluation. “We can customize what we want to see and prioritize everything according to the seven standard security levels of the DOD [Department of Defense].”

The NCDOC solution can easily customize information—by region or type of system, for example—and scale to meet increasing volumes of data. The Sentinel interface remains consistent, despite the addition of more sensors. The NCDOC team can also operate the Sentinel system from other locations, so the solution has no central point of failure.

“It would have been impossible to keep up with the dramatic increase in network security activity without at least 10,000 personnel,” said Granger. “Sentinel gives our centralized monitoring team a comprehensive and holistic view of security events, so we can immediately act on what is most critical.”

Sentinel also simplifies daily reporting with its ability to generate reports in all levels of detail for different audiences, whether commanders, other agency partners or joint security task forces. “As a government customer, we have high expectations,” said Rohwer.

Results
With Sentinel as part of its PROMETHEUS system, NCDOC has automated and centralized security monitoring for thousands of sensors across multiple, geographically dispersed networks. The ability to prioritize security events allows NCDOC to focus on events that require the most attention, such as network events aboard a ship entering a battle zone.

NCDOC can now create real-time reports in minutes or hours, instead of weeks or months. Because network security is vital to the nation’s defense, this information is a top priority for military leaders at the highest levels.

“Our job 24-7 is to secure and defend Navy networks worldwide against a persistent and adaptive threat. Sentinel helps us accomplish that,” said Granger. “The biggest military advantage is the power of information. We rely on the security of our networks to get the right information to the right people quickly.”